

Europäisches Patentamt European Patent Office Office européen des brevets



(11) **EP 0 645 912 A3**

(12)

EUROPEAN PATENT APPLICATION

(88) Date of publication A3: **12.01.2005 Bulletin 2005/02**

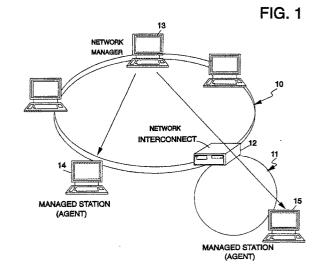
(51) Int CI.⁷: **H04L 12/24**, H04L 29/06, H04L 9/32

- (43) Date of publication A2: 29.03.1995 Bulletin 1995/13
- (21) Application number: 94480052.3
- (22) Date of filing: 21.06.1994
- (84) Designated Contracting States: **DE FR GB**
- (30) Priority: 25.08.1993 US 112007
- (71) Applicant: International Business Machines
 Corporation
 Armonk, N.Y. 10504 (US)
- (72) Inventors:
 - Augustine, Kurt Ernest Rochester, MN 55902 (US)

- Neeley, James Edward Sr Chapel Hill, NC 27514 (US)
- Strole, Norman Clark Raleigh, NC 27612 (US)
- (74) Representative: de Pena, Alain et al Compagnie IBM France Département de la Propriété Intellectuelle 06610 La Gaude (FR)

(54) Communication network access method and system

(57)A network management frame contains a clear text (unencrypted) management command field and a security field. The management frame is sent to a data communications network by an authorized managing entity (manager) (13). The management frame is addressed to a managing agent (agent) (14,15). The security field includes two sub fields. The first sub field is a clear text time stamp. The second sub field includes this same time stamp value concatenated with a checksum that is calculated by the manager for the specific clear text management command contained within the management frame. The concatenated value is then encrypted under a secret cryptographic key that is shared by the manager and the agent. The agent receives the management frame, calculates a checksum of the clear text management command, and appends this checksum to the clear text time stamp as contained in the received management frame. This value is then encrypted using the shared cryptographic code. If the result matches the second sub field of the received management command, integrity of the received management command is assured. Next, the clear text value of time stamp contained within the received management command is checked against a common clock within the agent. If the value of this time stamp falls within a predetermined time window, the authenticity of the received management command has been verified.





EUROPEAN SEARCH REPORT

Application Number EP 94 48 0052

	Citation of document with inc	ERED TO BE RELEVANT	Relevant	CLASSIFICATION OF THE	
Category	of relevant passag		to claim	APPLICATION (Int.Cl.6)	
X	J. GALVIN, K.MCCLOGI Protocols for versic Network Management I IETF DRAFT - NETWOR 1446, 1 April 1993 1-51, XP015007233 * page 2, line 1 - 1 * page 12, line 31 * page 38, line 1 -	1-18	H04L12/24 H04L29/06 H04L9/32		
A	TSUDIK G ED - INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: "Message authentication with one-way hash functions" ONE WORLD THROUGH COMMUNICATIONS. FLORENCE, MAY 4 - 8, 1992, PROCEEDINGS OF THE CONFERENCE ON COMPUTER COMMUNICATIONS (INFOCOM), NEW YORK, IEEE, US, vol. VOL. 2 CONF. 11, 4 May 1992 (1992-05-04), pages 2055-2059, XP010062203 ISBN: 0-7803-0602-3 * the whole document *		1-18	TECHNICAL FIELDS SEARCHED (Int.CI.6) H04L	
	The present search report has b	een drawn up for all claims			
	Place of search	Date of completion of the search	' 	Examiner	
The Hague 4 Novembe		4 November 2004	Gav	riliu, B-A	
CATEGORY OF CITED DOCUMENTS X: particularly relevant if taken alone Y: particularly relevant if combined with another document of the same category A: technological background O: non-written disclosure P: intermediate document		E : earlier patent doc after the filing date er D : document cited in L : document cited in	T: theory or principle underlying the invention E: earlier patent document, but published on, or after the filing date D: document cited in the application L: document cited for other reasons &: member of the same patent family, corresponding		